



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,752	03/18/2004	Peng T. Ong	59995-8009.US01	6881
22918	7590	07/03/2007		
PERKINS COIE LLP P.O. BOX 2168 MENLO PARK, CA 94026			EXAMINER NALVEN, ANDREW L	
			ART UNIT 2134	PAPER NUMBER
			MAIL DATE 07/03/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/803,752

Applicant(s)

ONG ET AL.

Examiner

Andrew L. Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 April 2007.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) 12-18 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11 and 19-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 July 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>3/13/2006</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-21 are pending.

Election/Restrictions

2. Claims 12-18 withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 16 April 2007.

Claim Objections

3. Claims 9-10 are objected to because of the following informalities:
4. Claim 9 contains a typo and should read, "the response is generated using a public-key cryptographic algorithm."
5. Claim 10 contains a typo and should read, "generated using a symmetric key cryptographic algorithm."
6. Appropriate correction is required.

Claim Rejections - 35 USC § 112

Art Unit: 2134

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1 and 9-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The cited claims are indefinite because it is unclear how the step of "decrypting the response" as defined in claim 1 is completed. Claim 1 provides that the response is decrypted using a user encrypted private key. Decrypting using an encrypted private key is incompatible with claim 9's encrypting of the challenge with the user's private key. If the challenge was encrypted using the user's private key then the decrypting of claim 1 could only be with the user's public key. Further, claim 1's decrypting using a user private key also is incompatible with claim 10's encryption with a shared secret because if the challenge was encrypted with a shared secret then decryption could only be with the shared secret.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2134

8. **Claims 1-5, 10 and 19-21 are rejected under 35 U.S.C. 102(e)** as being anticipated by Metral US PGPub 2004/0083296.

9. **With regards to claims 1 and 19 (as best understood)**, Metral teaches a method of operating an access system including a network access server to provide access between a user and a service network, the method comprising (Metral, paragraph 0027, user request for access to dial up network) providing an authentication server (Metral, paragraph 0027, server 204), generating a challenge using a random sequence without communicating with the network access server (Metral, paragraph 0027, encryption or tagging, paragraph 0029, uses two factor authentication with passcode that changes every 60 seconds), generating a response to the challenge (Metral, paragraph 0033, after embedding an encryption process is applied to the credential with embedded characteristic), sending the response to the network access server using an authentication protocol (Metral, paragraph 0033, credentials are sent from the user desktop client 201 to the client 202), forwarding the response to the authentication server (Metral, paragraph 0035, sent from the client 202 to the server), receiving and processing the response indicating whether the user is allowed access to the service network by decrypting the response using a user encrypted private key (Metral, paragraph 0037, seeks a match to allow access, paragraph 0023, authenticator includes the share of the shared secret).

10. **With regards to claim 2**, Metral teaches a challenge generated based on time (Metral, paragraph 0029, uses a pass code that changes every 60 seconds).

Art Unit: 2134

11. **With regards to claim 3**, Metral teaches the challenge is generated based on a non-repeating number sequence (Metral, paragraph 0029, pass code changes every 60 seconds).

12. **With regards to claim 4**, Metral teaches the authentication protocol being an indirect authentication protocol (Metral, paragraph 0033, RADIUS is an indirect authentication protocol).

13. **With regards to claim 5**, Metral teaches the authentication protocol is RADIUS (Metral, paragraph 0033-34, RADIUS encryption process).

14. **With regards to claim 10**, Metral teaches the response is generated using symmetric cryptographic algorithm and encrypting the challenge with a shared secret (Metral, paragraph 0032, symmetric stream ciphers).

15. **With regards to claim 20**, Metral teaches the user response including a random number decrypted using a user private key (Metral, paragraph 0029, pass code changes every 60 seconds, paragraph 0037, seeks a match to allow access, paragraph 0023, authenticator includes the share of the shared secret).

16. **With regards to claim 21**, Metral teaches the user response including a non repeating number sequence decrypted using a user private key (Metral, paragraph 0029, pass code changes every 60 seconds, paragraph 0037, seeks a match to allow access, paragraph 0023, authenticator includes the share of the shared secret).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

17. **Claims 6-8 are rejected under 35 U.S.C. 103(a)** as being unpatentable over

Metral US PGPub 2004/0083296 in view of Fink et al US PGPub 2004/0236702.

18. **With regards to claim 6**, Metral fails to teach the use of the TACAS

authentication protocol. However, Fink teaches the use of the TACAS authentication protocol (Fink, paragraph 0065, TACACS). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Fink's method of using TACAS with Metral's authentication method because it offers the advantage of offering a well known basic authentication protocol that provides both authorization and authentication that works with both local AAA and roaming situations (Fink, paragraph 0065).

19. **With regards to claim 7**, Metral fails to teach the use of the TACAS+

authentication protocol. However, Fink teaches the use of the TACAS+ authentication protocol (Fink, paragraph 0065, TACAS+). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Fink's method of using TACAS+ with Metral's authentication method because it offers the advantage of offering a well known basic authentication protocol that provides both authorization and authentication that works with both local AAA and roaming situations (Fink, paragraph 0065).

Art Unit: 2134

20. **With regards to claim 8**, Metral fails to teach the use of the XTACAS authentication protocol. However, Fink teaches the use of the XTACAS authentication protocol (Fink, paragraph 0065, XTACAS). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Fink's method of using XTACAS with Metral's authentication method because it offers the advantage of offering a well known basic authentication protocol that provides both authorization and authentication that works with both local AAA and roaming situations (Fink, paragraph 0065).

21. **Claims 9 and 11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Metral US PGPub 2004/0083296 in view of Ting US PGPub 2002/0174348.

22. **With regards to claim 9**, Metral fails to specifically teach the response is generated using public-key cryptographic algorithm and encrypting the challenge with the user's private key. However, Ting teaches the response is generated using public-key cryptographic algorithm and encrypting the challenge with the user's private key (Ting, paragraph 0035, challenged signed using a secret key of a public key/private key combination). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ting's method of encryption with Metral's authentication method because it offers the advantage of allowing strong authentication using at least two authentication factors which increases security (Ting, paragraph 0006).

Art Unit: 2134

23. **With regards to claim 11**, Metral as modified teaches the user's private key is stored in a smart card device (Ting, paragraph 0035, smart card is inserted and private key is utilized).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/803,752

Page 9

Art Unit: 2134

Andrew Nalven

An